

Re: Escalation of privilege

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-11/1178.html>

From: Torgeir Bakken (MVP) (*Torgeir.Bakken-spam_at_hydro.com*)

Date: 11/18/03

Date: Tue, 18 Nov 2003 23:57:31 +0100

Nicolas Macarez wrote:

- > *Hi Torgeir*
- > *Many thanks for your tiny tool – but great in my case.*
- > *It works, of course, but a new problem turn up: it's not the registry of*
- > *the current user which is modified but the registry of the Administrator*
- > *account – and it's not fine at all.*
- >
- > *In fact, runas open an admin session behind the scenes, executes the scripts*
- > *(and so modifies the HKEY_CURRENT_USER stuff, but the Administrator account*
- > *itself), and at last closes the session and gives you back the cursor.*
- > *The HKEY_CURRENT_USER of the plain current user (the guy with no admin*
- > *rights) is not modified at all.*
- >
- > *I'm still searching for a workaround...*

Hi

At least one of the buy-products can do this it looks like:

>From <http://www.netexec.de/>

<quote>

Temporary Administrator group memberships

Another feature that make NetExec a excellent choice for software installation scenarios are extended group memberships. Using this feature it is possible to run a process under a non-privileged user account, but inside this process the user becomes also a member of the Administrators group. Therefore the app uses the profile, settings and home directory of the non-privileged user account, but runs with Administrator privileges.

</quote>

--

torgeir

Microsoft MVP Scripting and WMI, Porsgrunn Norway

Administration scripting examples and an ONLINE version of the 1328 page

Scripting Guide: <http://www.microsoft.com/technet/scriptcenter>